CZU: [005.5:005.334](478)
DOI: https://doi.org/10.53486/icspm2023.05

OPERATIONAL RISK MANAGEMENT OF AN ENTERPRISE: ASSESSMENT AND MINIMIZATION METHODS

CAMINSCHI Olga
ORCID: 0000-0003-0854-2237
Master's degree, ASEM, olga.caminschi@mail.ru
DOROGAIA Irina
ORCID: 0000-0003-4625-8616
Conf.univ.,dr., ASEM, dorogaia.irina.ion@ase.md

ABSTRACT. *The relevance of the topic. In today's highly competitive and dynamic business environment, risk management has become a crucial factor for any organization's success. Operational risk, which includes all business processes, is an all-encompassing risk that needs to be addressed by organizations. However, given the current geopolitical situation and low levels of risk culture in Moldovan enterprises, operational risk management is becoming more critical than ever. To address this issue, the authors of a recent study analyzed the possible factors contributing to the emergence of operational risk in Moldovan enterprises, as well as methods for managing it. The study delved into various risk assessment techniques, risk mitigation measures, and risk transfer strategies to identify the most effective approaches to managing operational risk. By exploring the best practices and methods for minimizing operational risk, the study aimed to provide Moldovan enterprises with valuable insights and tools to improve their risk management practices.*

KEYWORDS: *operational risk, losses, assessment, mitigation, risk-management, competitiveness.*

JEL CLASSIFICATION: *M190*

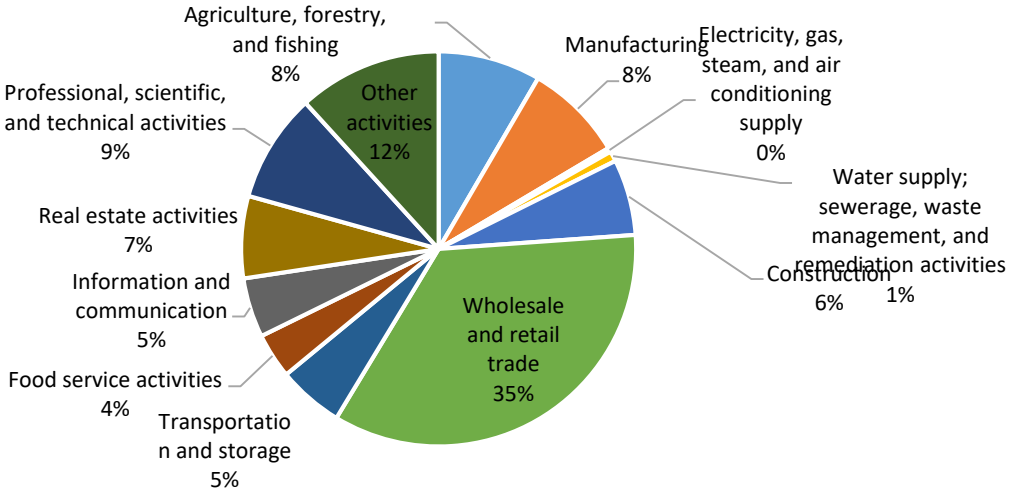
INTRODUCTION

In rapidly changing and complex business environment, organizations must constantly strive to minimize the impact of inherent risks. To achieve this, risk management has become a critical success factor for any economic unit. Enterprises must develop comprehensive strategies to manage different types of risks effectively. Risks are very diverse and very unpredictable, but at the same time, by classifying them and isolating the factors of influence, it is possible to manage them.

Given the fast-evolving nature of the external environment and the growing complexity of business operations, risk management must be prioritized as a critical component of an organization's strategic planning process. Effective risk management enables enterprises to optimize their business processes, minimize losses, and enhance their competitiveness. To achieve this, organizations must adopt a comprehensive risk management approach. By adopting a proactive approach to risk management, enterprises can identify potential risks before they arise, develop appropriate risk management strategies, and minimize the impact of any potential losses. Depending on the field of origin, there are many types of risks inherent in any organization, including (Table 1):

Table 1. Types of risks

Risk Name	Characteristics
Operational Risk	The risk, which affects the organization in many ways: can be associated with poor internal processes, system failure, the actions of staff, under the influence of external factors that may adversely affect the effectiveness of the organization
Legal Risk	Risk cases involving non-compliance with applicable laws, regulations, leading to loss of reputation, image, and financial loss.
Financial Risk	A variety of factors leading to loss of funds, investments, assets, income, currency, i.e., in which financial resources are involved.



Credit Risk	The risk, as a result of which the debtor cannot settle his obligations
Reputational Risk	Risks associated with loss of credibility and deterioration of the company's image, which may affect its competitiveness and, consequently, its financial results

Source: elaborated by the authors based on: [1,2,3]

For achieving competitiveness, an important stage for any organization is the early identification and evaluation of risks. This stage involves identifying potential factors that can affect the company's activities and lead to unfavorable situations. One of the risks that requires constant monitoring is operational risk. It involves the occurrence of losses resulting from inadequate internal processes, employee actions, systems or external factors. This risk affects the operational activities of enterprises and affects all business processes of the organization.

Therefore, managing operational risk is one of the most important priorities for ensuring uninterrupted processes of the organization and achieving maximum profits by minimizing costs and losses. The importance and relevance of the research topic are determined by the following:

- The variability of the external environment in which the organization operates;
- The rapid development of information technologies and the Internet of Things;
- The geopolitical situation in the Republic of Moldova;
- Development of entrepreneurship as the most important part of the country's economy.

It is well known that the culture of entrepreneurship, in particular, and risk management is at a very low level. Therefore, ***the aim of the study*** is to identify the main methodological directions for the study of operational risks in the enterprises of the Republic of Moldova and to develop appropriate measures to prevent unforeseen events associated with these risks. To achieve the research goal, the following priorities were formulated:

- Study of the conceptual features of operational risks,
- Studying the characteristics of the operating activities of enterprises in the Republic of Moldova, and the factors affecting them,
- Refinement of the algorithm for assessing and managing operational risks,
- Development of recommendations for managing operational risks.

I.THEORETICAL ASPECTS OF OPERATIONAL RISK

One of the complex objectives of the national development strategy of the Republic of Moldova 2030 is the development of the entrepreneurial sector within the framework of compliance with the principles of free competition and favorable market conditions. According to data from the National Bureau of Statistics for 2021, there are 59,4 thousand registered organizations (SMEs). Figure 1 shows the segmentation of organizations by direction of activity with the share of the total number of enterprises.

Figure 1. Share of SMEs in 2021 by main types of economic activity

Source: https://statistica.gov.md/ro/statistic_indicator_details/22#data_bank

Based on the provided data, the largest number of active enterprises is registered in the wholesale and retail sector. The share of enterprises in this sector is 35%, second largest sector is represented by agriculture - 8%. Regardless of the field of activity, any organization is subject to the influence of operational risk. In order to conduct a study on applicable practices for assessing and minimizing risk, was used induction methods, which involves identifying the most suitable method for managing operational risk based on the factors of occurrence. In addition, the method of analyzing statistical data, as well as experimental method, allowed to determine the most vulnerable business lines of the organization.

Operational risk represents the risk of incurring losses as a result of inadequate internal processes, employee actions, systems, or external factors.[1] Table 2 presents categories of types of operational risk events and assessment methods [4,5,6].

Table 2. Categories of operational risk events

Categories of Operational Risk Event Types*, *according to Basel II*	• Internal Fraud
	• External Fraud
	• Employment Practices and Workplace Safety
	• Clients, Products, and Business Practices
	• Damage to Physical Assets
	• Business Disruption and System Failures
	• Execution, Delivery, and Process Management
Methods for Assessing Operational Risk*, *according to Basel II*	• Basic Indicator Approach
	• Standardized Approach
	• Advanced Approaches, including: Internal Measurement Approach Loss Distribution Approach Scenario-Based Approach Judgmental Approach or Score-Based Approach

Source: elaborated by the authors conform [5,6]

The operational risk management system is complex, comprehensive and multi-component. Therefore, its stages can vary, but at the same time there is a certain algorithm of necessary steps:

- Identification and assessment of categories of sources of operational risks;
- Compilation of business process maps of the organization;
- Assessment of risk factors at the level of specific business processes;
- Identification of operations with a high level of risk;
- Development and implementation of measures to reduce identified critical risk areas;
- Implementation of control tools for vulnerable areas;
- Optimization of existing business processes taking into account risk exposure.

In the context of corporate risk management, there are using the three lines of defense model, which involves a balanced approach in defining the roles and responsibilities of all participants in the risk management system. The main role in making decisions regarding risk management lies with the process owner, who is involved in the daily implementation and management of this process. The second line of defense identifies risks that arise in daily operations and ensures the availability of necessary concepts, documents, and tools for managing risks. The third line of defense involves an independent and objective evaluation of existing risk management methods. Despite being a widespread model, this approach has drawbacks. Firstly, the first line of defense often feels excessive control, duplicated by the second and third lines,

[1] Basel Committee on Banking Supervision: Principles for the Sound Management of Operational Risk, 2011

leading to time constraints on current business tasks. In addition, there are cases where the first line stops performing control actions, believing that it is the responsibility of the second line. During a crisis, organizations often apply excessive control measures, creating additional tasks for the second and third lines. It is very important to prevent spontaneous reactions in such situations.

II.ASSESSMENT AND MINIMIZATION TOOLS

One of the tools for assessing an organization's level of operational risk is the method of determining and monitoring key risk indicators [7,8]. At the initial stage, are identified responsible functions. In each department are determined risk coordinators (first line of defense), who together with a second line of defense employee assess the existing business processes of the department. The first stage involves identifying potential risk factors that may lead to the realization of operational risk events. Then are determined potential KRIs, methodologies for their calculation, and monitoring frequency. The threshold value of key risk indicators is established in accordance with three zones:

- Green zone - an acceptable zone, where the risk is considered acceptable and no additional action is required.
- Yellow zone - a zone of increased attention, which requires action to return the indicator to the green zone.
- Red zone - a zone of immediate action.

It is worth noting the importance of pre-developed action plans when KRIs reach the yellow and red zones. For this purpose, second line of defense employees are responsible for developing the methodology (presented in internal regulatory acts), training responsible departments of companies in the basics of risk management, conducting joint review of key risk indicators to establish the adequacy of the applied practices. Key KPIs are developed and approved by the top management and the board of the company. Table 3 shows an example of risk indicators and possible actions in case the risks fall into the yellow and red zones.

Table 3. Examples of key risk indicators (KRI)

Indicator	Threshold value * 1	Threshold value* 2	Threshold value*3
Staff turnover	<3%	5%<= x <10%	>10%
Action plan when exceeding TV1,2		Analyze the reasons for the increased employee turnover; Review existing motivational packages to retain employees; Report information to the organization's management	Analyze the reasons why Plan 1 was ineffective; Apply new methods to attract potential employees; Report information to the organization's management
Internal fraud	0	1<= x <3	>= 3
Action plan when exceeding TV1,2		Analyze to identify vulnerable areas; Add control points	Apply new mechanisms to detect internal fraud; Report information to the organization's management

*Source: elaborated by the authors (*Thresholds are set as an example)*

Establishment of threshold limit zones is based on statistical data from past periods, taking into account forecasted expectations for the future. Threshold values and action plans when yellow and green zones are exceeded are approved by the management board and communicated to risk coordinators and department heads. It should be noted that the main role of key risk indicators is to warn in advance of the increased likelihood of operational risk events.

Another tool for assessing the level of operational risk in an organization is the process of self-assessment of risks and controls. This method involves assessing all business processes of the unit to identify existing risks. A distinctive feature of this process is that the owner of the process/product conducts the risk assessment. In other words, risk coordinators identify potential risk factors in the business process and existing control measures. To ensure the most effective conduct of the self-assessment process, the authors suggest following the algorithm [6,7,8]:

1. Develop a methodology and other internal regulations that regulate the process of conducting self-assessment;
2. Refine the steps of the comprehensive self-assessment plan, taking into account time periods, participants in the process, and other necessary aspects;
3. Approval of the developed plan by the organization's management;
4. Conduct a kick-off meeting with participants in the process to familiarize them with the principles and methodology of the process. Conduct training sessions;
5. Develop a self-assessment questionnaire that includes at least the following:
   - Identification of business processes of the unit;
   - Inherent risks that may arise;
   - Existing control measures.

6.Determine the frequency and impact of inherent risk on the enterprise's activities (in monetary terms).

7. Determine residual risk, which is calculated as the difference between inherent risk and the impact of risk control measures:

Residual risk = Initial risk - Impact of risk control measures

8. Depending on the size of the residual risk, priority areas are identified for developing action plans to minimize residual risk.

9. For better visualization, can be created a heat map that graphically displays the distribution of risks depending on the level of impact and frequency.

The final stage of the risk self-assessment process is to make a report for the enterprise's management to approve the developed action plans in accordance with priority. In case of unclear definition of the organizational structure of the enterprise or low risk culture, the authors recommend conducting training and other educational sessions to clarify the goal and clearly distribute the responsibilities of the participants in the process.

In the current geopolitical situation in the Republic of Moldova, the role of scenario planning as a risk management method increases. In particular, in the case of the operational risk, several scenarios are developed, with different variants of outcomes. This method involves studying the losses from operational risk that may arise as a result of implementing different scenarios. The essence of scenario analysis is to model situations that have a low probability of occurring but have significant consequences. The chosen scenario sets parameters for changing operations and the average size of losses for each type of activity, which in turn proportionally affects the assessment of the average frequency of events and losses. Depending on the chosen scenario, the calculation of capital for operational risk is carried out. The geopolitical situation that has emerged in Ukraine demonstrates the need for scenario analysis of various macroeconomic events. Figure 2 shows an analysis of the import and export of goods to the Republic of Moldova for the period of 2017-2022.

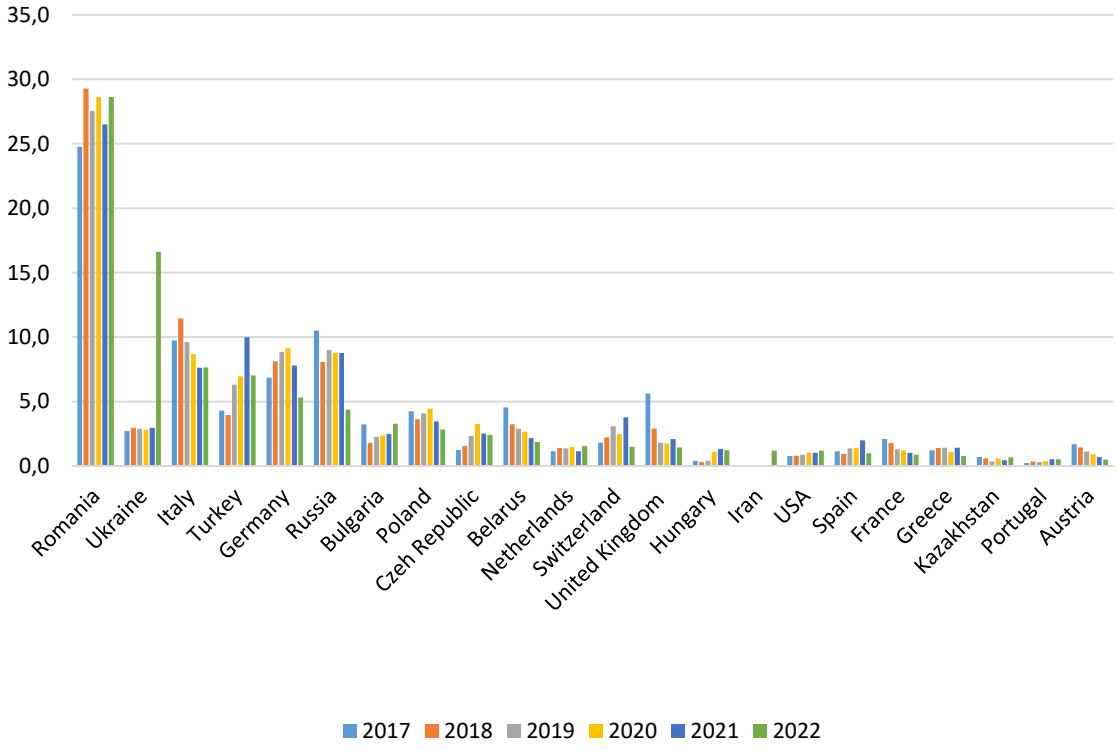


Figure 2. Export of goods of the Republic of Moldova for the period of 2017-2022.
Source: https://statistica.gov.md/ro/comertul-international-cu-marfuri-al-republicii-moldova-in-luna-decembrie-2022-s-9539_60309.html

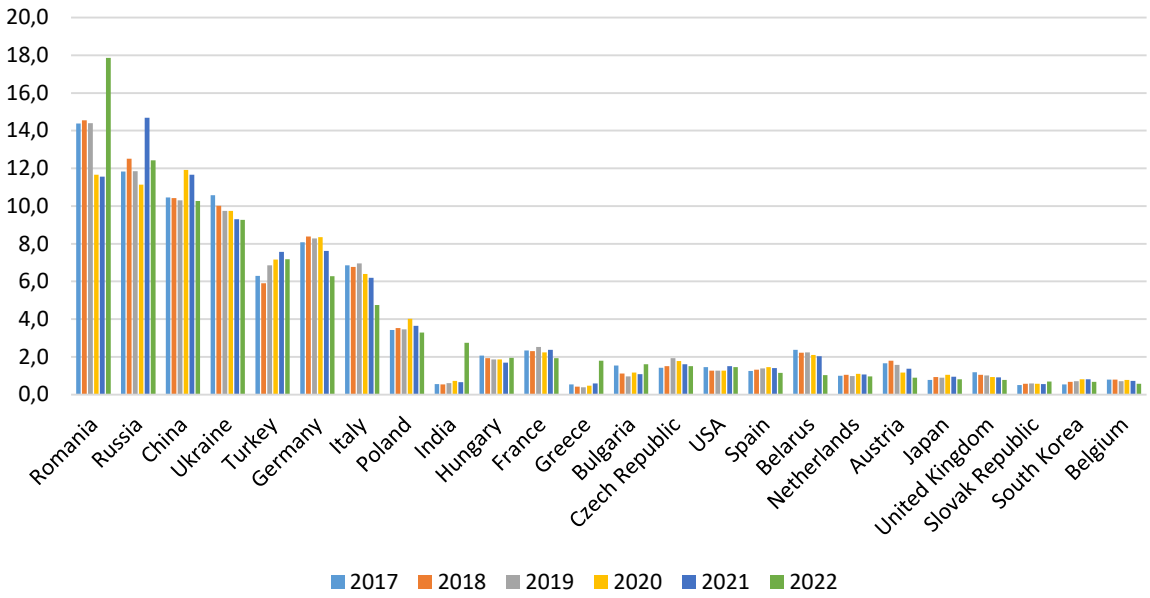


Figure 3. Import of goods to the Republic of Moldova for the period of 2017-2022.
Source: https://statistica.gov.md/ro/comertul-international-cu-marfuri-al-republicii-moldova-in-luna-decembrie-2022-s-9539_60309.html

As can be seen from the presented diagrams, Ukraine ranks 4th and 2nd among importing and exporting countries, respectively, accounting for 9.3% and 16.6%. Therefore, the inability to import or export goods is one of the scenarios that organizations should have foreseen in advance. Additionally, this has also impacted the availability of labor resources as well as other macroeconomic indicators that directly or indirectly increase the level of operational risk for enterprises.

The matrix, or risk map, is a widespread method of graphical representation of risks, taking into account the probability of occurrence of an event and the magnitude (scale) of its consequences. Usually, the risk map is presented as a rectangular table, with cells reflecting expected losses over a given time period. The coordinates of the cells correspond to the specified ranges of the frequency of adverse events over a given time period on one axis, and the specified ranges of the magnitude of losses resulting from the occurrence of an adverse event on the other. Fig. 4 is a figurative representation of the risk map, where they are logically combined in terms of probability of occurrence and hazard level

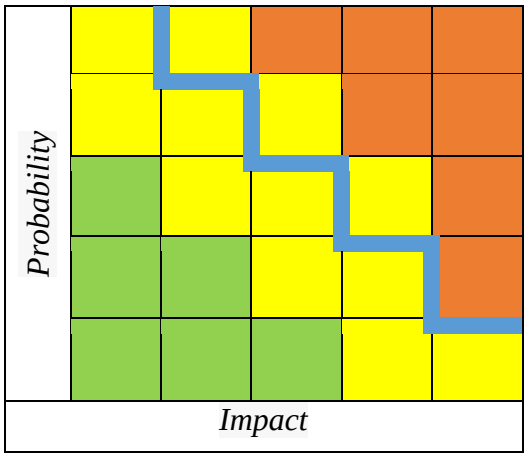


Figure 4. Figurative representation of the risk matrix
Source: elaborated by the authors aaccording to numerous studies [1,2,4,5,6]

For development of such map it is necessary to use the statistical data on frequency of occurrence of operational risk, usually with a periodicity for one year, at consideration of

frequency of occurrence of events connected with this risk. It is also possible to use external data, i.e., data on OR events that occurred in other organizations. Such data can be used for the purpose of calculating OR exposure only after adaptation to the specifics of the organization's activities, for which scaling mechanisms are applied.

CONCLUSIONS

Managing operational risk is a complex system that includes methods for identifying risk factors and ways to minimize them. To achieve competitiveness in current conditions, effective risk management of organizations is necessary. During the research, the following was identified by the authors:

- ✓ Enterprises in the Republic of Moldova have a low-risk culture that needs to be developed;
- ✓ To assess the level of operational risk, several different tools need to be applied simultaneously;
- ✓ Scenario analysis should be conducted in the current geopolitical environment;
- ✓ Operational risk is closely related to other types of organizational risk.

Based on the findings, the authors recommend:

Table 4. Authors' recommendations

Area	Recommendations
Risk culture enhancement	Conduct training sessions for the organization's personnel on risk culture Engage external organizations to conduct training sessions on risk culture enhancement Review organizational culture to make necessary changes
Risk factor identification	Apply all listed risk assessment tools in collaboration with the second line of defense, work together at all stages
Operational risk reporting	Record all risks and factors affecting them, depending on the level of management
Operational risk incidents registry	Develop and implement an operational risk incident registry with familiarization and entry access for all employees (depending on position), but with limited editing access.
Communication	Establish an effective information-sharing process regarding operational risks to obtain feedback and eliminate communication barriers.

Source: elaborated by the authors

Through communication among employees at different levels of the line of defense, it is possible to establish common risk management concepts and increase the effectiveness of the used tools. To achieve this, it is necessary to provide continuous training for personnel and develop the organizational culture of the enterprise. Thanks to effective risk management, enterprises in the Republic of Moldova will be able to increase their competitiveness both on the local and international levels.

REFERENCES

1. Alexander, C. (2003). *Operati1onal Risk: Regulation, Analysis and Management.* Avaiable: https://www.researchgate.net/publication/343110927_Analysis_of_Demand_Risks_for_the_Indian_Automotive_Sector_in_Globally_Competitive_Environment (acces date: 02.04.2023)

2. Amin, Z. (2016). *Quantification of operational risk: A scenario-based approach.* North American Actuarial Journal Avaiable: https://www.researchgate.net/publication/302634762_Quantification_of_Operational_Risk_A_Scenario-Based_Approach (acces date: 08.04.2023)

3. Dorogaia, I. (2016) *Особенности управления внутренними рисками при реализации инновационной деятельности предприятия***.** În: „25 de ani de reformă economică în Republica Moldova: prin inovare și competitivitate spre progres economic”, Conferința Științifică Internațională din 23-24 septembrie 2016, Chișinău, ASEM, 2016, vol. I, p. 215-219, 0,25 c.a., ISBN 978-9975-75-837-6. Avaiable:: https://old.ase.md/files/publicatii/electronice/Conf_2016_Vol_1.pdf (acces date: 09.04.2023)

4. Dutta, K., & Babbel, D. F. (2014). *Scenario Analysis in the Measurement of Operational Risk Capital: A Change of Measure Approach. Journal of Risk and Insurance,* 81 (2), 303-334. Avaiable: http://dx.doi.org/10.1111/j.1539-6975.2012.01506.x/abstract (acces date: 03.04.2023)

5. BCBS. (2001). *Operational risk. Supporting document to the New Basel Capital Accord*. Basel Committee on Banking Supervision, Consultative Document. Available: https://www.bis.org/publ/bcbsca07.pdf. (acces date: 10.04.2023)

6. BCBS. (2011). Operational risk. Supervisory guidelines for the advanced measurement approaches. Basel Committee on Banking Supervision. Available: www.bis.org/publ/bcbs196.htm. (acces date:08.04.23)

7. Segal, T. (2023) Operational Risk Overview, Importance, and Examples. Available: https://www.investopedia.com/terms/o/operational_risk.asp (acces date: 11.04.2023)

8. Eceiza J.& Kristensen I. (2020) The future of operational-risk management in financial services. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services (acces date: 11.04.2023)